Лапець О.В., асистент

Дмитренко М.В., студент

ДНУ ім. О. Гончара, м. Дніпро

ORCID:  [0000-0002-7707-3588](https://orcid.org/0000-0002-7707-3588)  Olha Lapets

**ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ**

У світі, де інформація стала найбільш цінним активом, захист інформаційних систем стає докучливо актуальним завданням. Необхідність захищати дані від кіберзлочинців, внутрішніх загроз та недоліків у програмному забезпеченні настільки велика, що вимагає постійної уваги та інноваційних підходів.

 Кіберзагрози постійно розвиваються та ускладнюються. До основних типів кібератак належать:

* Фішинг - це атака, в якій зловмисники використовують підроблені електронні листи або веб-сайти для обману користувачів та отримання їхніх особистих даних.
* Зловмисне програмне забезпечення - це програмне забезпечення, яке розроблено для заподіяння шкоди комп'ютерам або мережам.
* Атаки на мережі - це атаки, спрямовані на порушення роботи мережі або крадіжку даних, що передаються по мережі.

Для захисту від кібератак використовуються різні заходи, такі як:

* Захист доступу - це заходи, спрямовані на обмеження доступу до інформаційних систем лише авторизованим користувачам.
* Шифрування - це процес перетворення інформації в незрозумілий для сторонніх осіб формат.
* Антивірусне програмне забезпечення - це програмне забезпечення, яке виявляє та видаляє зловмисне програмне забезпечення [1].

Недоліки у програмному забезпеченні є однією з основних причин кібератак. Вразливості у програмному забезпеченні можуть бути використані зловмисниками для отримання доступу до систем або крадіжки даних.

Для виявлення та усунення вразливостей у програмному забезпеченні використовуються різні методи, такі як:

* підтвердження безпеки
* безпека розробки .

Недостатня усвідомленість щодо безпеки - це одна з основних проблем у сфері кібербезпеки. Користувачі часто не знають про кібератаки та не вживають заходів для захисту своєї інформації.

Для підвищення обізнаності користувачів про кібербезпеку використовуються різні заходи, спрямовані на інформування користувачів про кібератаки .

Інформаційна безпека в освіті - це важлива проблема, оскільки освітні установи зберігають велику кількість конфіденційної інформації про студентів, викладачів та співробітників.

Для забезпечення інформаційної безпеки в освіті використовуються різні заходи, такі як:

* Освіта та тренінги для студентів, викладачів та співробітників - це заходи, спрямовані на підвищення обізнаності про кібербезпеку.
* Впровадження систем управління кібербезпекою - це заходи, спрямовані на управління кібербезпекою в освітній установі [2].

Для захисту інформаційних систем, які використовуються в управлінні проектами і програмами, використовуються різні заходи, такі як:

Впровадження систем управління кібербезпекою - це заходи, спрямовані на управління кібербезпекою в проекті або програмі.

Освіта та тренінги для учасників проекту або програми - це заходи, спрямовані на підвищення обізнаності про кібербезпеку .

Розвиток штучного інтелекту (ШІ) викликає нові виклики у сфері кібербезпеки. ШІ може бути використаний для створення нових кібератак, які є більш складними та ефективними.

Для захисту від кібератак, які використовують ШІ, використовуються різні заходи, а саме:

* Розробка нових методів виявлення та протидії кібератак - це заходи, спрямовані на розробку нових методів, які можуть виявити та протистояти кібератакам, які використовують ШІ.
* Розвиток нових методів шифрування - це заходи, спрямовані на розробку нових методів шифрування, які є більш стійкими до атак, які використовують ШІ.

Проблеми захисту у сучасних інформаційних системах є складними та різноманітними. Розв'язання цих проблем вимагає комплексного підходу, який включає в себе як технічні, так і організаційні заходи .

**Література**

1. Дудатьєв А. В.Захист комп’ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с.
2. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.